INFORMATION TECHNOLOGY DEPARTMENT

Bismarck, North Dakota

INFORMATION SYSTEM AUDIT

For the Year ended December 31, 2007

Project Code SAI112-07

TABLE OF CONTENTS

May 30, 2008

Honorable John Hoeven, Governor
Members of the Legislative Assembly
Lisa Feldner, Chief Information Officer, Information Technology Department

Transmitted herewith is the general controls audit of the Information Technology Department as of December 31, 2007. The North Dakota Century Code states that the State Auditor “be vested with the duties, powers, and responsibilities involved in performing the post audit of all financial transactions of the state government, detecting and reporting any defaults, and determining that expenditures have been made in accordance with law and appropriation acts.” Audits of the state’s information systems are an important part of these responsibilities.

The audit of the Information Technology Department general controls disclosed three reportable conditions. Each of these reportable conditions will be explained in detail within this report.

Inquiries or comments relating to this audit may be directed to Donald LaFleur, Information Systems Audit Manager, by calling (701) 328-4744. We wish to express our appreciation to the Information Technology Department for the courtesy, cooperation, and assistance provided to us during this audit.

Sincerely,

Robert R. Peterson
State Auditor

EXECUTIVE SUMMARY

This report is intended to provide interested parties with information sufficient to understand the general controls of the Information Technology Department (ITD) for the period January 1, 2007 to December 31, 2007.

General controls encompass the environment in which all applications are processed. Their purpose is not typically directed to any one application, but to all applications processed at the data center. Effective general controls provide the proper environment for good application controls.

The report is structured according to guidance from the American Institute of Certified Public Accountants' statement of auditing standards number 70 as amended. In accordance with these standards, we obtained a description of controls from ITD and performed testing to ensure the controls were in place and were operating effectively.

Our audit resulted in the following significant findings:

- ITD has not tested the Disaster Recovery Plan. (page 26)
- ITD lacks a formal Security Plan. (page 29)
- ITD lacks a formal risk assessment framework. (page 44)

INDEPENDENT AUDITOR'S REPORT

Honorable John Hoeven, Governor
Members of the Legislative Assembly
Lisa Feldner, Chief Information Officer, Information Technology Department

We have examined the accompanying description of controls related to the general controls of the Information Technology Department (ITD). Our examination included procedures to obtain reasonable assurance about whether (1) the accompanying description presents fairly, in all material respects, the aspects of ITD's controls that may be relevant to a state agency's internal control as it relates to an audit of financial statements, (2) the controls included in the description were suitably designed to achieve the control objectives specified in the description, if those controls were complied with satisfactorily and state agencies applied the controls contemplated in the design of ITD's controls, and (3) such controls had been placed in operation as of December 31, 2007. The control objectives were specified by the management of ITD.

Our audit did not include vulnerability assessment or penetration testing as those objectives were performed under contract with an outside firm and that report was issued under separate cover.

Our examination was performed in accordance with standards for information system audits issued by the Information Systems Audit and Control Foundation, applicable Government Auditing Standards issued by the Comptroller General of the United States, and standards established by the American Institute of Certified Public Accountants. Our examination included those procedures we considered necessary under the circumstances to obtain a reasonable basis for rendering our opinion. We believe that our audit provides a reasonable basis for our opinion.

ITD states in its description of controls that it tests the continuity plan yearly. Our tests of operating effectiveness noted that the continuity plan has not been tested since the recovery site was moved to Mandan. This resulted in the nonachievement of the control objective "Ensure Continuous Service".

In our opinion, except for the matter described in the preceding paragraph, based on our audit, the accompanying description of the aforementioned general controls presents fairly, in all material respects, the relevant aspects of ITD's controls that had been placed in operation as of December 31, 2007. Also, in our opinion, the controls, as described, are suitably designed to provide reasonable assurance that the specified control objectives would be achieved if the described controls were complied with satisfactorily and state agencies applied the controls contemplated in the design of ITD's controls.

In addition to the procedures we considered necessary to render our opinion as expressed in the previous paragraph, we applied tests to specific controls, listed in the Information Provided by the State Auditor's Office, to obtain evidence about their effectiveness in meeting the control objectives described in the Information Provided by the State Auditor's Office during the period from January 1, 2007 to December 31, 2007. Any projection of such information to the future is subject to the risk that, because of change, the description may no longer portray the controls in existence. The potential effectiveness of specific controls at ITD is subject to inherent limitations and, accordingly, errors or fraud may occur and not be detected. Furthermore, the projection of any conclusions, based on our findings, to future periods is subject to the risk that (1) changes made to the system or controls, (2) changes in processing requirements, or (3) changes required because o the passage of time may alter the validity of such conclusions.

This report is intended solely for use by the Governor, Legislative Audit and Fiscal Review Committee, ITD, state agencies, and auditors of the state agencies and is not intended to be and should not be used by anyone other than those specified parties.

Robert R. Peterson
State Auditor

May 30, 2007

BACKGROUND INFORMATION

North Dakota Century Code Section 54-59-02 states "The information technology department is established with the responsibility for all wide area network services planning, selection, and implementation for all state agencies, including institutions under the control of the board of higher education, counties, cities, and school districts in this state. With respect to a county, city, or school district, wide area network services are those services necessary to transmit voice, data, or video outside the county, city, or school district. In exercising its powers and duties, the department is responsible for computer support services, host software development, statewide communications services, standards for providing information to other state agencies and the public through the internet, technology planning, process redesign, and quality assurance. The department may not exercise its powers and duties in a manner that competes or otherwise interferes with the provision of telecommunications service to a private, charitable, or nonprofit entity by a privately or cooperatively owned telecommunications company."

North Dakota Century Code Section 54-59-05 states the department:

1. Shall provide, supervise, and regulate information technology of all executive branch state entities, excluding the institutions under the control of the board of higher education.

2. Shall provide network services in a way that ensures the network requirements of a single entity do not adversely affect the functionality of the whole network, facilitates open communications with the citizens of the state, minimizes the state's investment in human resources, accommodates an ever-increasing amount of traffic, supports rapid detection and resolution of problems, protects the network infrastructure from damage and security breaches, provides for the aggregation of data, voice, video, and multimedia into a statewide transport mechanism or backbone, and provides for the network support for the entity to carry out its mission.

3. May review and approve additional network services that are not provided by the department.

4. May purchase, finance the purchase, or lease equipment, software, or implementation services or replace, including by trade or resale, equipment or software as may be necessary to carry out this chapter. An agreement to finance the purchase of software, equipment, or implementation services may not exceed a period of five years. The department shall submit any intended financing proposal for the purchase of software, equipment, or implementation services under this subsection, which is in excess of one million dollars, to the budget section of the legislative council or the legislative assembly before executing a financing agreement. If the budget section or the legislative assembly does not approve the execution of a financing agreement, the department may not proceed with the proposed financing arrangement. The department may finance the purchase of software, equipment, or implementation services only to the extent the purchase amount does not exceed seven and one-half percent of the amount appropriated to the department during that biennium.

5. Shall review requests for lease, purchase, or other contractual acquisition of information technology as required by this subsection. Each executive branch agency or institution, excluding the institutions under the control of the board of higher education, shall submit to the department, in accordance with guidelines established by the department, a written request for the lease, purchase, or other contractual acquisition of information technology. The department

shall review requests for conformance with the requesting entity's information technology plan and compliance with statewide policies and standards. If the request is not in conformance or compliance, the department may disapprove the request or require justification for the departure from the plan or statewide policy or standard.

6. Shall provide information technology, including assistance and advisory service, to the executive, legislative, and judicial branches. If the department is unable to fulfill a request for service from the legislative or judicial branch, the information technology may be procured by the legislative or judicial branch within the limits of legislative appropriations.

7. Shall request and review information, including project startup information summarizing the project description, project objectives, business need or problem, cost-benefit analysis, and project risks and a project closeout information summarizing the project objectives achieved, project budget and schedule variances, and lessons learned, regarding any major information technology project of an executive branch agency, the state board of higher education, or any institution under the control of the state board of higher education as provided in section 54-35-15.2. The department shall present the information to the information technology committee on request of the committee.

8. May request and review information regarding any information technology project of an executive branch agency with a total cost of between one hundred thousand and two hundred fifty thousand dollars as determined necessary by the department. The department shall present the information to the information technology committee on request of the committee.

9. Shall study emerging technology and evaluate its impact on the state's system of information technology.

10. Shall develop guidelines for reports to be provided by each agency of the executive, legislative, and judicial branches, excluding the institutions under the control of the board of higher education, on information technology in those entities.

11. Shall collaborate with the state board of higher education on guidelines for reports to be provided by institutions under control of the state board of higher education on information technology in those entities.

12. Shall review the information technology management of executive branch agencies or institutions.

13. Shall perform all other duties necessary to carry out this chapter.

14. May provide wide area network services to a state agency, city, county, school district, or other political subdivision of this state. The information technology department may not provide wide area network service to any private, charitable, or nonprofit entity except the information technology department may continue to provide the wide area network service the department provided to the private, charitable, and nonprofit entities receiving services from the department on January 1, 2003. The department shall file with the state auditor before September 1, 2003, a description of the wide area network service the department provided to each private, charitable, and nonprofit entity receiving services from the department on January 1, 2003.

15. Shall assure proper measures for security, firewalls, and internet protocol addressing at the state's interface with other facilities.

16. Notwithstanding subsection 14, may provide wide area network services for a period not to exceed four years to an occupant of a technology park associated with an institution of higher education or to a business located in a business incubator associated with an institution of higher education.

OBJECTIVES, SCOPE, AND METHODOLOGY

Audit Scope

This report is intended to provide interested parties with information sufficient to understand the general controls in place within the Information Technology Department (ITD) during the period from January 1, 2007 to December 31, 2007. This report has been prepared taking into consideration the guidance contained in the AICPA Statement on Auditing Standards No. 70 as amended.

Our audit was conducted in accordance with the *Standards for Information Systems Auditing* issued by the Information Systems Audit and Control Association and *Government Auditing Standards* issued by the Comptroller General of the United States.

Audit Objectives

The objective of this audit was to ensure that controls listed in the Description of Controls were in place and operating effectively.

DESCRIPTION OF CONTROLS

Human Resource Controls

ITD uses the ND Human Resource Management Services division job classifications for all positions, which detail the minimum qualifications necessary for each position. A position information questionnaire (PIQ) is used to further define the position qualifications and personnel selection criteria.

ITD recruitment practices include participating at technical expos and college job fairs, advertising available positions on the ITD and Central Personnel web-sites, as well as in the print media and with Job Service of North Dakota.

ITD performed criminal background checks on all employees and recorded fingerprints in June 2003. ITD performs an annual update of the employee information and has defined procedures to perform follow-up background checks on the employees every five years. The Bureau of Criminal Investigations is contracted to perform this service for ITD.

On an annual basis, ITD employees are required to sign an Acknowledgment of Secrecy Provision to ensure they are aware of the confidentially requirements of the data they handle. In addition there is an annual acknowledgement of seven other policies relevant to the department.

ITD management is committed to personnel training and career development. Employee training is the responsibility of the employee and their manager. ITD division managers may specify training needs in an employee's annual evaluation or approve requests for training submitted by the employee. Training requests, status, and costs are tracked internally. Training costs are tracked by section, and averaged by FTE for budget tracking/estimating purposes.

ITD surveys internal employees to identify and assess any performance issues and establish internal goals / objectives.

ITD will pay for the testing required for professional certifications and upon completion will provide a one-time bonus to the employee.

ITD employee resignation procedures follow a documented exit process to return keys, door access cards, and all ITD equipment. Account privileges, email and voicemail services are disabled upon resignation.

ITD issues a pre-action notice to employees subject to termination, and places the employee on administrative leave. The employee must return keys, door access cards, and all ITD equipment. Account privileges, email and voicemail services are disabled upon resignation or termination notice.

ITD policies and procedures are published and made available to ITD employees on the intranet.

ITD follows the NDCC and policies developed by OMB regarding annual leave accrual and cut-off dates for leave balances above 240 hours.

ITD's Human Resources Division has established policies and procedures for the evaluation and re-evaluation of IT position descriptions.

ITD's Human Resources Division maintains policies and procedures in accordance with applicable laws and regulations.

ITD procedures ensure that ongoing cross-training and backup of staff for critical job functions occurs.

Contingency Planning Controls

ITD maintains a disaster recovery hotsite in Mandan, ND. The hotsite facility provides replication of critical data and selected application servers. It houses full daily backup tapes for file recovery or complete system restoration.

ITD performs a yearly test of the Disaster Recovery Plan at the hotsite facility. Tests include restoring the IBM S/390 mainframe, AS/400, and UNIX system platforms, and establishing the network / communications with the disaster recovery site. Test procedures and results are documented and reviewed by ITD's Contingency Planning Specialist, who coordinates any necessary changes to the Disaster Recovery Plan.

ITD's disaster recovery tests provide for a mix of experienced and non-experienced personnel involvement on each recovery test. External agency personnel also participate in the testing process to validate recovery of their applications.

ITD's off-site storage facility includes a back-up of the current operating system, system/390 (mainframe) start-up instructions, one copy of the disaster recovery plan, and a recovery priority list of mainframe and mid-tier applications. A copy of the back-up tapes is kept at the off-site storage facility.

ITD's off-site storage facility is physically secured through a combination vault door and cement walls and ceiling. There are no windows and only a small vent for air conditioning. There is a fire extinguisher located inside the off-site vault. There are no formal annual inspections; however, ITD personnel use the vault daily. ITD updates the vault combination upon every employee turnover, or annually at a minimum.

ITD's Contingency Planning Specialist is responsible for establishing and maintaining ITD's disaster recovery plan through participation in the Continuum of Government Team, formed in June 2002, headed by the Office of Management and Budget - Risk Management Division. This team is tasked with establishing a uniform web-enabled relational database software application from Strohl Systems Group, Inc. - Living Disaster Recovery Planning System (LDRPS).

ITD maintains a consistent philosophy and framework over business contingency plan development and prioritizes internal and statewide applications with respect to criticality and timeliness of recovery, as mandated by the Continuum of Government Team, through criteria listed in the LDRPS system.

ITD defines specific roles and responsibilities over continuity planning within the LDRPS and determines the specific test, maintenance and update requirements for the contingency plan.

ITD's disaster recovery plan maintained in LDRPS includes the following:
- Emergency procedures to ensure the safety of staff members, as required by the COG Team.
- Roles & Responsibilities including team members and leaders, task assignments, vendor and customer contact information, administrative support personnel, and site-specific personnel.
- Identification of all software applications required to restore a business function and the recovery time objective (RTO) for each application.
- Administrative functions for communicating and providing support services such as benefits, payroll, and external communications.
- Specific equipment and supply needs.
- Training / awareness of individual and group roles.
- Itemization of contract service providers, services, and response expectations.
- Logistical information on location of key resources such as O/S, applications, data files, operating manuals, etc.
- Current contact information of key personnel.
- Business resumption alternate work locations for all users once IT resources are available.

ITD ensures agency requirements over continuity planning are met and coordinates with four primary agencies (Bank of North Dakota, Department of Transportation, Department of Human Services and Tax Department) to identify specific federal regulatory requirements. ITD works with those agencies to meet the requirements.

User Agency Control – Contingency Planning

Agencies should work with ITD for their data and applications to ensure ITD includes them as appropriate in ITD's contingency plan.

ITD's contingency plan, outlined in LDRPS, includes the identification of resources needed to recovery a business function. ITD cross trains employees to perform various disaster recovery tasks.

ITD's data center, network operations center, and second data center run off of UPS and have back up power generators.

Security Controls

ITD's Administrative Services Division has formally assigned to a security officer organization wide responsibility for formulation of internal control and security (logical and physical) policies and procedures.

All data and systems in the custody of ITD have a defined owner. The defined owner is the agency responsible for the business results or the business use of the object. There is one and only one owner for each object.

User Agency Control – Data Owner Responsibility

The owning agency appoints an agency security officer who is responsible for controlling access rights.

ITD maintains logical security access controls at the mainframe and mid-tier platform levels and maintains a history of user id operating system level access. Controls include:
- Invalid sign on attempt lockout
- Unauthorized attempts to access system resources
- Resource access privileges by user id (mainframe)
- Authorized security definitions and rule changes
- History of up to 5 passwords and limits on password reuse.
- Password standards, as defined by the Enterprise Architecture Security Domain Team, are implemented at the mainframe and mid-tier operating system

ITD, through the Enterprise Architecture Security Domain Team, has implemented policies and procedures to address:
- Prevention and detection of computer viruses, and installation of virus prevention software and critical updates.
- Firewall intrusion prevention and detection mechanisms over the state network environment, including proactive intrusion detection and passive review of intrusion attempts
- Business-only use of computer resources, including fax and voice mail
- Remote access

ITD enforces Windows Active Directory standards internally, over user authentication within their internal Windows and web-based applications. Agency security personnel are responsible for establishing and monitoring active directory parameters, in accordance with EA Security Domain Team recommendations, for user authentication and data access privileges within their own directories of the state network.

ITD has implemented information authentication and integrity standards over networked resources through Active Directory, thereby providing a single network sign-on within a single network domain. ITD provides the Domain controllers and Global Catalog servers for authentication services.

ITD's Network Firewall Group supports maintenance of firewalls based upon authorized service requests passed through the Work Management System after review by the ITD Security division. ITD's policy rules over firewall control is to "lock down all, and open up to only authorized hosts that require access" rather than "allow all, except for”.

ITD's Security team reviews firewall activity logs each following business day for reported "failed connection" attempts. The review looks for repeated attempts to break one or multiple firewalls within the network - if found, the Security Officer reports the incident(s) to the Network Firewall Group to lock the offender from accessing the outermost state network firewall.

Active Directory login credentials are encrypted during transmission.

ITD deploys SSL encryption where appropriate.

ITD has implemented Intrusion Detection Systems and performs regular vulnerability assessments on its computing and network infrastructure.

ITD has a formal incident response policy and team that is used when responding to security related incidents.

ITD utilizes an on-line Work Management System where authorized users can request adds, changes or deletes to access rights for systems maintained by ITD.

User Agency Control – Controlling User Access

Agencies should:

- Develop policies and procedures for adding, changing, and removing employee access
- Review daily access violation reports and follow-up with ITD when needed
- Review access rights for employees and all applications periodically

On an annual basis, ITD contacts the Security Officers at each agency to review the access rights granted to each agency. This is an addition to the daily and monthly access reports sent to each agency.

ITD's Computer Operations Team maintains the RACF and SMF central database security software that controls access to agency-owned datasets, library files, source code, etc. ITD Computer Operations Team also administers the Work Management System (WMS) via DBA's, as well as the internal security tools for general level access auditing within SQL-server and Oracle databases. Note: Agencies are responsible for establishing the internal controls and business process over data input, processing, and output for transaction activity conducted at the agency site.

The Highway Patrol provides maintenance and security of the capitol complex, including the offices and facilities of ITD.

ITD's Security Officer supports the Highway Patrol administration procedures as specific to ITD.

ITD has locked facilities and requires all employees, contractors and visitors to wear identification badges while on the ITD premises.

Operating Controls

ITD's Computer Facility environmental controls include fire suppression, raised floors, water detectors, smoke alarms and air conditioning units. Semi-annual tests are done to verify correct alarm operation. Facility Management Division provides a UPS for back-up power and power regulation, and a generator for extended power loss. The UPS is tested semi-annually and the generator is tested weekly.

ITD's Computer Facility includes a separate agency server room where agencies can store their network / application servers. The severs are backed up and ITD assumes maintenance of the server operating system. Agency personnel may obtain limited access to the agency server room from ITD security personnel.

ITD's Computer Facility agency server room has a raised floor, smoke detectors, air conditioning, and security camera. Agency personnel are allowed access to the room through their key cards.

ITD schedules mainframe / mid-tier operating system down-time with agency IT coordinators, posts the outage schedule on the website, and provides web-based subscription service for automated email notifications of future scheduled maintenance activities.

ITD monitors computer and network operations performance based on assessments of individual systems and the knowledge of support and project teams, tools such as graphs, operators’ knowledge, and available performance capacity system software. Performance management reports include e-mail messages by platform for e-mail servers, CPU utilization, DASD I/O per second, memory pages per second, and disk capacity for the mainframe.

ITD's mainframe and AS/400 platforms include redundant hardware controls to ensure continued operations in event of a part failure. In addition, the mainframe O/S software will contact IBM technical service support as necessary.

ITD critical servers have redundant power supplies and all disk systems utilize RAID to ensure no data lass due to hard drive failures.

ITD’s computer operations include instructions for operators such as checklists, IPL instructions, shut down procedures, restart procedures, on-call lists, console commands, and other miscellaneous memos.

ITD uses Operations Planning and Control Scheduler (OPC) to schedule nightly jobs on the mainframe. Production control employees or agency personnel can schedule jobs in OPC. Production control specialists review the nightly job schedules. Jobs that abend (abnormally end) will send a message to the mainframe master console. Operators will then contact on call programmers and responsible agency personnel to fix the job.

ITD computer operations utilizes IBM’s Syslog (System Log) to log activity on the mainframe.

ITD completed deployment of the Work Management System (WMS) to state agency users in November 2004. ITD developed this web-based system internally to provide a "one-stop center" for customers to request ITD software development services, and enhance ITD's project management, time recording, and billing services.

ITD has implemented Mercury SiteScope infrastructure monitoring software over the state network platform to monitor performance characteristics (utilization, response time, usage and resource availability). ITD has configured SiteScope to automatically detect and report/record incidents over network resources.

ITD's Computer Systems Division has implemented ongoing procedures to monitor performance and capacity of the mainframe and mid-tier operating systems within the computer facility, and maintains historical statistics for future capacity planning and budgetary planning purposes.

ITD's Computer Systems Division maintains the configuration inventory (hardware, O/S software, applications software, facilities and data files) through HP's Systems Insight Manager software configuration tools, Altiris and the CIS Database (ITD application for hardware).

ITD's Computer Systems Division utilizes Quest Stat Application Change Management (ACM) for PeopleSoft tools for patch management, versioning capabilities, process management and change request tracking over the ConnectND application. Other QA/change control/developer tools include IBM's Rational ClearCase and Cool:Gen

ITD's Computer Systems Division database administrators use the Work Management System to track customer change requests and document software changes over Websphere, .NET, and agency database applications maintained by ITD.

ITD's Computer Systems Division manages desktop computer configurations using Altiris Client Management Suite tools for desktop and notebook computers. In accordance with ITD Policy DT002-04.1, the Altiris Client Management Suite provides the ability to connect, load software, load patches, do troubleshooting, and get asset information from a remote site. Records of installed software may be obtained through Altiris. ITD's "acceptable use policy" addresses unauthorized software installations on state-owned computers by employees.

ITD validates the software installed on mainframe / midtier / desktop platforms agrees to the licensed inventory when renewing annual maintenance agreements with the vendor.

ITD provides physical security, backup/recovery, O/S maintenance services, and production processing services for agency applications that reside in the Computer Operations Facility. Agencies are responsible for managing their data processed through the applications. ITD provides the scheduling software agencies may use to schedule regular job runs. System output printed at ITD's computer facility is secured from unauthorized access.

ITD's Production Control team provides production processing services for agency applications residing in the computer facility. These include: production control reports through CA:Librarian, central print and storage of system output until picked up by authorized agency personnel, maintenance of IBM's Syslog for 6 months, transfer and handling of agency inventory media, "zero-ing" of all hard drives for all desktops and other internal drives.

ITD's Magstar - Librarian and LTO 3 Library tape backup systems include automated cleaning and write verification processes.

ITD's Computer Operations and Production Control teams ensure operations are adequately managed by maintaining and/or following documented operational instructions, managing and evaluating performance statistics over hardware and peripheral capacity utilization and performance, ensuring equipment is maintained on schedule, and ensuring a physical and logical segregation of source and object, test / development / production libraries.

ITD manages changes to application software by documenting, prioritizing, and tracking system changes requests from users. The change process is monitored by ITD for improvements in acknowledgment, response time, response effectiveness and user satisfaction with the process.

ITD utilizes a formal SDLC methodology to develop and maintain applications for its customers. This methodology includes peer reviews and load testing for quality assurance purposes.

ITD Distributed Systems utilizes a web-based change management system to log changes. Changes are logged in the system and approved by the Computer Systems Manager or the System Architect.

ITD utilizes separate test and production environments critical systems. Some systems have separate development environments as well. New applications or application changes are tested by users in the separate test platform or region. After acceptance ITD system administrators and/or DBA migrate the changes to production.

Manage Problems and Incidents

ITD's Customer Service Division Support Center operates a help desk and provides a full-service central repository for customers to report problems, ask questions, request information, and receive back resolutions and answers in an organized and expedient manner.

ITD's Customer Service Division staff includes the Customer Service Director, Service Center Manager, one full-time Service Management Software Analyst and five full-time Service Desk Analysts. Service Desk Analysts cover 7am - 5pm M-F and rotate on-call Saturday morning through Monday 7am. Computer Operations staff cover calls 5pm - 7am M-F.

ITD's Support Center receives requests via telephone and email, and logs / tracks the requests through HEAT from FrontRange Solutions - Incident Management System. ITD has implemented HEAT with the following control parameters:
- Defined assignment groups, supervisors, and role-specific security
- Defined incident categories, call-types, sub-call-types, and incident priority matrix
- Defined detail screens to gather call-type specific information, and customer-specific details
- Acknowledgement, escalation, and communication procedures
- Monthly reporting & analysis, incident records archived 3 years

ITD's Customer Service Division performs monthly reporting and analysis of incident records (HEAT) and Automatic Call Distribution (ACD) telephone system records, and tracks performance measures based upon key indicators.

ITD's Customer Service Division has implemented the Continuous Improvement Cycle based upon IT Infrastructure Library (ITIL) best practices for Service Desks, Incident Management, and Change Management.

ITD's Computer Systems Division utilizes HEAT incident tracking system to address issues - escalation procedures are being followed and appropriate in resolving problems.

Organizational Controls

ITD is divided into seven divisions (Administrative Services, Software Development, Computer Systems, Telecommunications, Customer Service, IT Planning, Human Resources) to ensure authority and independence from user organizations.

Appropriate roles and responsibilities exist for key processes, including system development life cycle activities, (requirements, design, development, testing), information security, acquisition and capacity planning.

ITD organizational controls ensure appropriate and adequate resources are assigned to implement the organization's policies in a timely manner.

Governance structures are in place to set the direction over the enterprise programs, CJIS, ConnectND and GIS.

ITD procedures exist to address the need to periodically review and approve key standards, directives, policies and procedures relating to information technology.

ITD management promotes a positive control environment by example and has accepted full responsibility for formulating, developing, documenting, promulgating, controlling and regularly reviewing policies governing general aims and directives.

ITD establishes the operating budget through the executive planning process (Budget Analysis & Reporting System) and manages budget v. actual expenditures through the centralized PeopleSoft accounting system. The budget is aligned with the enterprise strategic plan. Executive Branch agencies participate in preparing their portions of the IT plan. A goal of the process is to anticipate major infrastructure needs and plan accordingly.

The governor and state legislature set staffing levels biennially in ITD's budget. During the biennial budget process, ITD reviews staffing levels and requests additional FTE as needed.

ITD sets its rates to cover the cost of providing services with a reasonable surplus to finance capital purchases. ITD monitors actual expenditures to billings through the PeopleSoft accounting system cost centers with the goal of matching billings to expenditures within each cost center.

ITD rate setting process and annual report include comparisons to similar rates charged by other states and private sector providers to ensure that the rates are competitive with similar services offered by other states and the private sector.

ITD manages its legal and contractual responsibilities and liabilities through ongoing internal monitoring of legislation, contracts, and regulatory changes.

User Agency Control – Legal and Contractual Requirements

Agencies should inform ITD of legal and contractual requirements where ITD is responsible for compliance.

ITD performs and annual physical inventory of fixed assets within the department.

ITD obtains independent assurance of compliance with laws, regulatory requirements and contractual obligations through audit functions conducted by the Office of the State Auditor. The State Auditor performs routine examinations of ITD's financial, performance, and IT controls.

ITD's Procurement Officer reviews RFP's and contracts for compliance with policies and procedures over hardware and software acquisition, implementation, and maintenance. State procurement rules govern the acquisition process - acquisitions must comply with state standards unless an exception is granted.

ITD's works with OMB's Central Services Division to establish statewide contracts for selected IT hardware and software and has established a vendor pool for qualified firms to provide IT development and consulting services.

ITD utilizes the Attorney General standard contracts where possible, and has established service level agreements with key providers that provide contracted services to ITD. ITD's large-dollar contracts are reviewed and approved by the Attorney General. In addition, ITD follows the RFP and state procurement process.

ITD evaluates the internal control processes within the department on an ongoing basis, through management meetings, budgetary review, external audits - including SAS70 reviews, internal security assessment, and through internal assessment of policies and procedures.

ITD management and staff meet on a scheduled basis to discuss internal operations and direction. Managers and supervisors meet weekly, and all ITD staff meets twice per year.

IT Planning Controls

ITD publishes an annual report which includes: major accomplishments; ITD's performance against goals; ITD's service rates (rates that generate 90% of ITD revenue) which are compared with costs charged by similar organizations; the strategic planning process; an update on internal performance measures, and future IT initiatives. ITD distributes the report to the Legislative Information Technology Committee, Legislative Audit and Fiscal Review Committee and Senior Information Technology Committee. The report is also available at ITD's website under "Publications".

ITD publishes a quarterly agency newsletter titled "Information Link." ITD also coordinates the "IT Directional Meeting" for executive branch agency representatives to inform them on current initiatives and issues.

ITD conducts an annual customer survey to ensure the department is meeting customers' expectations. The survey allows customers to rate their satisfaction with the services provided by ITD and to suggestions for improvements. Survey areas are service desk, software development, network service, E-mail services, telephone services, application hosting, records management, IT planning and oversight services, and an overall ITD survey. Results are published in ITD's strategic plan and on ITD's website.

ITD meets with key customers on a monthly or quarterly basis to gather information about future plans and needs.

Per NDCC 54-59-07, the Statewide Information Technology Advisory Committee (SITAC) advises ITD regarding statewide IT planning, including providing e-government services for citizens and businesses, developing technology infrastructure to support economic development and workforce training, and developing other statewide IT initiatives and policy.

ITD has established an Enterprise Architecture process. This process relies on participation of agency representatives. Each agency that is interested is invited to participate in various domain teams that study specific technology domains and provide proposals to the Architecture Review Board (ARB) and State Information Technology Advisory Committee (SITAC). This process addresses enterprise technology issues and results in state standards, policies and guidelines.

ITD is legislatively mandated to develop policies, standards, and guidelines for technology based on information from state agencies, institutions, and departments with the goal of creating a common statewide architecture. The Enterprise Architecture (EA) process promotes state agency participation with ITD in setting future direction of information technology in the state of North Dakota.

User Agency Control – Compliance with IT Standards

A Compliance with Standards section is included in agency IT plans. Agencies indicate the status of their compliance with standards and policies and if not in compliance, provide an approved waiver request and provide plans to bring the agency into compliance.

ITD maintains a biennial Strategic Business Plan, outlining goals and objectives for the department, and follows a methodology for measuring progress toward the goals outlined in the business plan, per NDCC 54-59-06.

ITD evaluates progress toward the goals outlined in the strategic plan, and publishes the results in the annual report (balanced scorecard). ITD also tracks performance metrics internally, both at the department and division levels.

ITD's strategic planning process outlines the rates and funding mechanisms necessary to finance the proposed activities of the department, in accordance with NDCC 54-59-06.

ITD's strategic planning process takes into account organizational changes, technology evolution, regulatory requirements, business process reengineering efforts and staffing requirements.

ITD's technological infrastructure is maintained on an ongoing basis, takes into account current and future technology trends and regulatory conditions, and is compared with the IT long and short range plans.

ITD manages risks associated with individual procurement contracts based on the dollar value and by requiring agencies to provide documented requests for information technology.

ITD provides guidelines for agencies to follow in preparing their technology plan, reviewing the plans for compliance with statewide policies or standards, resolving conflicting directions among plans, and assembling the agency plans into a statewide plan to be submitted to the members of the Legislative Assembly. ITD also reviews and approves technology acquisitions for conformance with the agency's IT plan and compliance with statewide policies and standards.

State agency IT Plan updates are to be done as needed to communicate the IT direction and resource needs of the agency. The IT plan must be updated if the goals and objectives change, if a major project is added or deleted, or at the request of ITD.

User Agency Control – Prepare Budget Based on IT Plan

Each state entity is responsible for preparing its budget request based on its IT plan and must describe in detail how the IT plan relates to the budget request. Similarly, the executive budget recommendation must include detailed information about the relationship to the agency's IT plan.

ITD's annual customer survey includes a section on information technology planning. ITD's Information Technology Planning Analyst reviews the surveys and meets with agencies to assess the IT planning process.

Large Project Controls

North Dakota Century Code Section 54-35-15.2 provides that the Legislative Information Technology Committee shall "review the cost-benefit analysis of any major information technology project (=> 250K per biennium or => $500K in total) of an executive or judicial branch agency" and "perform periodic reviews to ensure that a major information technology project is on its projected schedule and within its cost projections."

ITD's large project reporting has five phases: business case, project plan, quarterly status reports, summary status report, and post-project analysis. In the business case phase the agency defines the business requirements, does a cost/benefit and risk analysis, establishes a project manager and executive steering team, and presents this to the Legislative Information Technology Committee. ITD has established guidelines for making the business case. The project plan is to be prepared based on industry "best practices." ITD encourages the use of the Project Management Institute (PMI) format. Quarterly reports define the scope of the project and state the project schedule. The report compares budgeted to actual costs and outlines current progress and issues. ITD's planning analysts review the report and present summary status reports to the Legislative Information Technology Committee each quarter. The post-project analysis assesses whether the project accomplished its business objectives.

ITD's large project oversight process ensures the project plan includes a formal system development life cycle for system development and installation, including requirements definition, coding, testing, conversion, training, and documentation.

ITD's large project oversight process incorporates quality management processes within the project plan.

INFORMATION PROVIDED BY THE STATE AUDITOR'S OFFICE

Objective – Managing Human Resources

To acquire and maintain a motivated and competent workforce and maximize personnel contributions to the IT processes.

Controls

ITD uses the ND Human Resource Management Services division job classifications for all positions, which detail the minimum qualifications necessary for each position. A position information questionnaire (PIQ) is used to further define the position qualifications and personnel selection criteria.

ITD recruitment practices include participating at technical expos and college job fairs, advertising available positions on the ITD and Central Personnel web-sites, as well as in the print media and with Job Service of North Dakota.

ITD performed criminal background checks on all employees and recorded fingerprints in June 2003. ITD performs an annual update of the employee information and has defined procedures to perform follow-up background checks on the employees every five years. The Bureau of Criminal Investigations is contracted to perform this service for ITD.

On an annual basis, ITD employees are required to sign an Acknowledgment of Secrecy Provision to ensure they are aware of the confidentially requirements of the data they handle. In addition there is an annual acknowledgement of seven other policies relevant to the department.

ITD management is committed to personnel training and career development. Employee training is the responsibility of the employee and their manager. ITD division managers may specify training needs in an employee's annual evaluation or approve requests for training submitted by the employee. Training requests, status, and costs are tracked internally. Training costs are tracked by section, and averaged by FTE for budget tracking/estimating purposes.

ITD surveys internal employees to identify and assess any performance issues and establish internal goals / objectives.

ITD will pay for the testing required for professional certifications and upon completion will provide a one-time bonus to the employee.

ITD employee resignation procedures follow a documented exit process to return keys, door access cards, and all ITD equipment. Account privileges, email and voicemail services are disabled upon resignation.

ITD issues a pre-action notice to employees subject to termination, and places the employee on administrative leave. The employee must return keys, door access cards, and all ITD equipment. Account privileges, email and voicemail services are disabled upon resignation or termination notice.

ITD policies and procedures are published and made available to ITD employees on the intranet.

ITD follows the NDCC and policies developed by OMB regarding annual leave accrual and cut-off dates for leave balances above 240 hours.

ITD's Human Resources Division has established policies and procedures for the evaluation and re-evaluation of IT position descriptions.

ITD's Human Resources Division maintains policies and procedures in accordance with applicable laws and regulations.

ITD procedures ensure that ongoing cross-training and backup of staff for critical job functions occurs.

Tests of Operating Effectiveness and the Results of Those Tests

We interviewed ITD personnel regarding hiring, training, and termination procedures.

We selected a sample of ten current employees to check that they had criminal background checks, had signed the yearly acknowledgement of understanding of ITD's policies and security responsibilities, had professional certifications appropriate for their position, and had received adequate training for their position.

ITD has a policy that a position will be filled within 60 days of it being requested. A selection process checklist has been created that lists all the steps taken in the hiring process. ITD advertises job openings on web sites and newspapers. For each different position, ITD has developed a system to rate the resumes that they receive. The rating is specific to the duties of each position. The interview team normally consists of one person from the Human Resources division, the division director of the position being filled, and the immediate supervisor of position being filled. Once a candidate is selected ITD does a reference check and background check (through Attorney General) are performed.

ITD leaves training needs to employees and their supervisors. Training received is tracked and recorded by ITD's HRMS division.

ITD developed a termination checklist that identifies who is responsible for each step. Each step is checked off and initialed when completed. For involuntary terminations, ITD increases their security level by locking all doors and requiring valid key cards to access them.

Our test of ten employees showed that all had criminal background checks, signed yearly acknowledgement of reading and understanding ITD policies and security responsibilities, had appropriate certifications for their position, and received appropriate training for their position during the audit period.

Conclusion

We conclude that ITD has met the objective of managing human resources.

Objective – Ensuring Continuous Service

To make sure IT services are available as required and to ensure a minimum business impact in the event of a major disruption.

Controls

ITD maintains a disaster recovery hotsite in Mandan, ND. The hotsite facility provides replication of critical data and selected application servers. It houses full daily backup tapes for file recovery or complete system restoration.

ITD performs a yearly test of the Disaster Recovery Plan at the hotsite facility. Tests include restoring the IBM S/390 mainframe, AS/400, and UNIX system platforms, and establishing the network / communications with the disaster recovery site. Test procedures and results are documented and reviewed by ITD's Contingency Planning Specialist, who coordinates any necessary changes to the Disaster Recovery Plan.

ITD's disaster recovery tests provide for a mix of experienced and non-experienced personnel involvement on each recovery test. External agency personnel also participate in the testing process to validate recovery of their applications.

ITD's off-site storage facility includes a back-up of the current operating system, system/390 (mainframe) start-up instructions, one copy of the disaster recovery plan, and a recovery priority list of mainframe and mid-tier applications. A copy of the back-up tapes is kept at the off-site storage facility.

ITD's off-site storage facility is physically secured through a combination vault door and cement walls and ceiling. There are no windows and only a small vent for air conditioning. There is a fire extinguisher located inside the off-site vault. There are no formal annual inspections; however, ITD personnel use the vault daily. ITD updates the vault combination upon every employee turnover, or annually at a minimum.

ITD's Contingency Planning Specialist is responsible for establishing and maintaining ITD's disaster recovery plan through participation in the Continuum of Government Team, formed in June 2002, headed by the Office of Management and Budget - Risk Management Division. This team is tasked with establishing a uniform web-enabled relational database software application from Strohl Systems Group, Inc. - Living Disaster Recovery Planning System (LDRPS).

ITD maintains a consistent philosophy and framework over business contingency plan development and prioritizes internal and statewide applications with respect to criticality and timeliness of recovery, as mandated by the Continuum of Government Team, through criteria listed in the LDRPS system.

ITD defines specific roles and responsibilities over continuity planning within the LDRPS and determines the specific test, maintenance and update requirements for the contingency plan.

ITD's disaster recovery plan maintained in LDRPS includes the following:
- Emergency procedures to ensure the safety of staff members, as required by the COG Team.
- Roles & Responsibilities including team members and leaders, task assignments, vendor and customer contact information, administrative support personnel, and site-specific personnel.
- Identification of all software applications required to restore a business function and the recovery time objective (RTO) for each application.

- Administrative functions for communicating and providing support services such as benefits, payroll, and external communications.
- Specific equipment and supply needs.
- Training / awareness of individual and group roles.
- Itemization of contract service providers, services, and response expectations.
- Logistical information on location of key resources such as O/S, applications, data files, operating manuals, etc.
- Current contact information of key personnel.
- Business resumption alternate work locations for all users once IT resources are available.

ITD ensures agency requirements over continuity planning are met and coordinates with four primary agencies (Bank of North Dakota, Department of Transportation, Department of Human Services and Tax Department) to identify specific federal regulatory requirements. ITD works with those agencies to meet the requirements.

ITD's contingency plan, outlined in LDRPS, includes the identification of resources needed to recovery a business function. ITD cross trains employees to perform various disaster recovery tasks.

ITD's data center, network operations center, and second data center run off of UPS and have back up power generators.

ITD's mainframe and AS/400 platforms include redundant hardware controls to ensure continued operations in event of a part failure. In addition, the mainframe O/S software will contact IBM technical service support as necessary.

ITD critical servers have redundant power supplies and all disk systems utilize RAID to ensure no data lass due to hard drive failures.

Tests of Operating Effectiveness and the Results of Those Tests

We examined ITD's disaster recovery plan.

We reviewed the results of the latest test of the disaster recovery plan.

We inspected the Mandan Data Center and backup site to ensure they contained the necessary information.

We interviewed ITD personnel regarding meetings with the four primary agencies. The quality and completeness of ITD's disaster recovery plan is dependent on these meetings and other agencies working with ITD to ensure their data and applications are properly included in ITD's disaster recovery plan.

We interviewed key personnel from the disaster recovery plan to ensure they were aware of the plan, understood their role, and had participated in training or testing of the plan.

ITD's disaster recovery plan contains the necessary information for proper recovery. ITD based their current disaster recovery plan on the Mandan Data Center.

ITD has not tested their disaster recovery plan since moving to the Mandan Data Center.

We verified that there was a copy of the disaster recovery plan in the backup site. The contingency planner stated that they keep a back-up of the current operating system, which is a snapshot of the mainframe. He stated that this is kept on tapes that are brought over to the backup site every Monday.

Minutes are not taken for the meetings with the four primary agencies. Discussions with ITD indicate that the meetings are not formal and are held only as needed.

Our interviews of key personnel indicated that the employees were aware of the disaster recovery plan, understood their roles, and the employees received training or participated in tests.

Finding: ITD has not tested the Disaster Recovery Plan

ITD has yet to perform a disaster recovery test on any platform in the Mandan Data Center since moving there in 2006. The IT continuity plan should be tested on a regular basis to ensure the IT systems can be effectively recovered, shortcomings are addressed and the plan remains relevant. ITD has been working on issues at the Mandan Data Center, they are waiting until the issues are fixed to perform the test. Without a test of the continuity plan the effectiveness of that plan is in question.

Recommendation

We recommend that ITD perform a disaster recovery test on a yearly basis.

ITD Response

ITD agrees with the recommendation and plans to perform regular testing of the infrastructure located at the second data center. Initial work at the second data center focused on ensuring that the data replication infrastructure was performing as anticipated and relocating the development/test environments for critical systems to enhance our ability to recover from incidents affecting our production systems. Since field work for the audit was completed ITD has performed testing for three of the critical systems with redundant hardware in place at the second data center.

Conclusion

We conclude that ITD has failed to meet the objective to ensure continuous service due to their failure to test their continuity plan.

Objective – Ensuring Systems Security

To safeguard information against unauthorized use, disclosure, modification, damage, or loss.

Controls

ITD's Administrative Services Division has formally assigned to a security officer organization wide responsibility for formulation of internal control and security (logical and physical) policies and procedures.

All data and systems in the custody of ITD have a defined owner. The defined owner is the agency responsible for the business results or the business use of the object. There is one and only one owner for each object - the owning agency appoints an agency security officer who is responsible for controlling access rights.

ITD maintains logical security access controls at the mainframe and mid-tier platform levels and maintains a history of user id operating system level access. Controls include:
- Invalid sign on attempt lockout
- Unauthorized attempts to access system resources
- Resource access privileges by user id (mainframe)
- Authorized security definitions and rule changes
- History of up to 5 passwords and limits on password reuse.
- Password standards, as defined by the Enterprise Architecture Security Domain Team, are implemented at the mainframe and mid-tier operating system

ITD, through the Enterprise Architecture Security Domain Team, has implemented policies and procedures to address:
- Prevention and detection of computer viruses, and installation of virus prevention software and critical updates.
- Firewall intrusion prevention and detection mechanisms over the state network environment, including proactive intrusion detection and passive review of intrusion attempts
- Business-only use of computer resources, including fax and voice mail
- Remote access

ITD enforces Windows Active Directory standards internally, over user authentication within their internal Windows and web-based applications. Agency security personnel are responsible for establishing and monitoring active directory parameters, in accordance with EA Security Domain Team recommendations, for user authentication and data access privileges within their own directories of the state network.

ITD has implemented information authentication and integrity standards over networked resources through Active Directory, thereby providing a single network sign-on within a single network domain. ITD provides the Domain controllers and Global Catalog servers for authentication services.

ITD's Network Firewall Group supports maintenance of firewalls based upon authorized service requests passed through the Work Management System after review by the ITD Security division. ITD's policy rules over firewall control is to "lock down all, and open up to only authorized hosts that require access" rather than "allow all, except for".

ITD's Security team reviews firewall activity logs each following business day for reported "failed connection" attempts. The review looks for repeated attempts to break one or multiple firewalls within the network - if found, the Security Officer reports the incident(s) to the Network Firewall Group to lock the offender from accessing the outermost state network firewall.

Active Directory login credentials are encrypted during transmission.

ITD deploys SSL encryption where appropriate.

ITD has implemented Intrusion Detection Systems and performs regular vulnerability assessments on its computing and network infrastructure.

ITD has a formal incident response policy and team that is used when responding to security related incidents.

ITD utilizes an on-line Work Management System where authorized users can request adds, changes or deletes to access rights for systems maintained by ITD.

On an annual basis, ITD contacts the Security Officers at each agency to review the access rights granted to each agency. This is an addition to the daily and monthly access reports sent to each agency.

ITD's Computer Operations Team maintains the RACF and SMF central database security software that controls access to agency-owned datasets, library files, source code, etc. ITD Computer Operations Team also administers the Work Management System (WMS) via DBA's, as well as the internal security tools for general level access auditing within SQL-server and Oracle databases. Note: Agencies are responsible for establishing the internal controls and business process over data input, processing, and output for transaction activity conducted at the agency site.

Tests of Operating Effectiveness and the Results of Those Tests

We reviewed IT standards related to security.

We reviewed yearly access rights confirmations sent to agencies.

We reviewed the ITD's Work Management System (WMS) for security requests. To properly notify ITD of security requests through WMS agencies should have policies and procedures for adding, changing, and removing their employee's access.

We reviewed ITD's incident response policy and intrusion detection system.

Enterprise Architecture Standards related to security include:

- Anti-Virus
- Remote Access
- Incident Response
- Active Directory
- State Government Network Security
- Access Control
- Encryption
- Auditing
- Employee Security Awareness
- Physical Access
- Public Workstation Access

- Anti-Spyware
- Mobile Device Access Control

ITD sends agencies listings of access rights from the following areas, agencies are to review, sign and return the listings to ITD.

- Mainframe OS Data Set Authorization Report
- Mainframe ADABAS Entire Network File Authorization Report
- Mainframe NATURAL File Authorization Report
- Mainframe DB2 Data Set Authorization Report
- Mainframe CICS Transaction Authorization Report
- Mainframe User ID Report
- AS/400 User ID Report
- Oracle User ID Report
- Password Change Information Report

All security requests are processed through ITD's Work Management System. Agencies prepare work orders and attach the appropriate security service requests to the work order and submit it to ITD. ITD retains the work orders in the Work Management System for an audit trail.

ITD operates a commercial intrusion detection system; a number of sensors are placed throughout the network to look for suspicious activity that is reported through the central system. In conjunction with this system ITD has a formal incident response policy that documents how ITD in conjunction with agencies will respond to network security incidents.

Finding: ITD lacks a formal Security Plan

Security plans are needed to provide centralized direction and control over information security. The lack of a formal security plan increases the risk that information security will not be consistently applied across the organization and increases the dependence on the expertise of current employees.

Recommendation

We recommend that ITD develop a security plan that provides centralized direction and control over information security.

ITD Response

ITD agrees with the recommendation and plans to develop a formal security plan. ITD does have dedicated security staff who focus on enterprise security issues and procedures, however we do agree that there is value in formalizing existing processes and standards into an overall plan.

Conclusion

We conclude that ITD has met the objective of ensuring system security. The findings and recommendations noted are meant to improve the level of security offered by ITD and do not, in our view; represent significant issues that would affect the overall assessment of system security at ITD.

Objective – Managing Facilities

To provide a suitable physical surrounding which protects the IT equipment and people against man-made and natural hazards.

Controls

The Highway Patrol provides maintenance and security of the capitol complex, including the offices and facilities of ITD.

ITD's Security Officer supports the Highway Patrol administration procedures as specific to ITD.

ITD has locked facilities and requires all employees, contractors and visitors to wear identification badges while on the ITD premises.

ITD's Computer Facility environmental controls include fire suppression, raised floors, water detectors, smoke alarms and air conditioning units. Semi-annual tests are done to verify correct alarm operation. Facility Management Division provides a UPS for back-up power and power regulation, and a generator for extended power loss. The UPS is tested semi-annually and the generator is tested weekly.

ITD's Computer Facility includes a separate agency server room where agencies can store their network / application servers. The severs are backed up and ITD assumes maintenance of the server operating system. Agency personnel may obtain limited access to the agency server room from ITD security personnel.

ITD's Computer Facility agency server room has a raised floor, smoke detectors, air conditioning, and security camera. Agency personnel are allowed access to the room through their key cards.

Tests of Operating Effectiveness and the Results of Those Tests

We reviewed ITD's physical security policy.

We toured ITD facilities to ensure adequate protections were in place for physical security and environmental monitoring.

We reviewed the latest fire inspection report for ITD facilities.

We interviewed personnel responsible for operating the key card system regarding its function and also reviewed related policies and procedures.

We tested access rights for key ITD facilities (computer room, Mandan data center, agency server room).

We reviewed the UPS and backup generator to ensure they provided adequate protection from power loss.

ITD facilities are protected by a key card system operated by Highway Patrol. Our review of access rights to the computer room, Mandan data center, and agency server room found that access was appropriate.

ITD has a Physical Security Policy which covers access controls, vendor access, and escorting of visitors.

ITD in accordance with OMB policy ITD conducts a yearly inventory.

Our tour of the computer room found that the necessary protections from fire, water, humidity, and temperature are in place in the computer room. Facilities Management monitors, tests, and maintains the environmental sensors and alarms.

The Mandan data center has smoke detectors, raised flooring, air conditioning, and temperature and humidity sensors (monitored by ITD). There are no water sensors under the flooring or fire suppression at this facility.

The backup facility is locked and contains humidity and temperature controls as well as fire detection. ITD monitors and logs temperature and humidity conditions daily.

The local fire department performs a yearly fire inspection of the entire capital building. They inspected ITD facilities in August 2008. No significant problems with ITD facilities were noted in the inspection reports.

Highway Patrol operates the key card system that protects ITD facilities. ITD is responsible for issuing and recovering key cards with its employees. ITD controls access rights for the doors to its facilities. ITD's Physical Security Policy covers ITD's responsibilities with the key card system.

There are sensors in the UPS room to monitor the environment. Facilities Management uses the same monitor software to monitor this room as they use to monitor the computer room and the agency server room. If the room gets too hot, the UPS shuts down and transfers the load to MDU. The system issues a high temperature warning at 78°F and shuts down the system at 85°F. The UPS and batteries are tested twice per year, generally in May and November.

Conclusion

We conclude that ITD has met the objective of managing facilities.

Objective – Managing Operations

To ensure that important IT support functions are performed regularly and in an orderly fashion.

Controls

ITD schedules mainframe / mid-tier operating system down-time with agency IT coordinators, posts the outage schedule on the website, and provides web-based subscription service for automated email notifications of future scheduled maintenance activities.

ITD's computer operations include instructions for operators such as checklists, IPL instructions, shut down procedures, restart procedures, on-call lists, console commands, and other miscellaneous memos.

ITD uses Operations Planning and Control Scheduler (OPC) to schedule nightly jobs on the mainframe. Production control employees or agency personnel can schedule jobs in OPC. Production control specialists review the nightly job schedules. Jobs that abend (abnormally end) will send a message to the mainframe master console. Operators will then contact on call programmers and responsible agency personnel to fix the job.

ITD computer operations utilizes IBM's Syslog (System Log) to log activity on the mainframe.

ITD's Computer Systems Division maintains the configuration inventory (hardware, O/S software, applications software, facilities and data files) through HP's Systems Insight Manager software configuration tools, Altiris and the CIS Database (ITD application for hardware).

ITD's Computer Systems Division utilizes Quest Stat Application Change Management (ACM) for PeopleSoft tools for patch management, versioning capabilities, process management and change request tracking over the ConnectND application. Other QA/change control/developer tools include IBM's Rational ClearCase and Cool:Gen

ITD's Computer Systems Division manages desktop computer configurations using Altiris Client Management Suite tools for desktop and notebook computers. In accordance with ITD Policy DT002-04.1, the Altiris Client Management Suite provides the ability to connect, load software, load patches, do troubleshooting, and get asset information from a remote site. Records of installed software may be obtained through Altiris. ITD's "acceptable use policy" addresses unauthorized software installations on state-owned computers by employees.

ITD validates the software installed on mainframe / midtier / desktop platforms agrees to the licensed inventory when renewing annual maintenance agreements with the vendor.

ITD provides physical security, backup/recovery, O/S maintenance services, and production processing services for agency applications that reside in the Computer Operations Facility. Agencies are responsible for managing their data processed through the applications. ITD provides the scheduling software agencies may use to schedule regular job runs. System output printed at ITD's computer facility is secured from unauthorized access.

ITD's Production Control team provides production processing services for agency applications residing in the computer facility. These include: production control reports through CA:Librarian, central print and storage of system output until picked up by authorized agency personnel, maintenance of IBM's Syslog for 6 months, transfer and handling of agency inventory media, "zero-ing" of all hard drives for all desktops and other internal drives.

ITD's Magstar - Librarian and LTO 3 Library tape backup systems include automated cleaning and write verification processes.

ITD's Computer Operations and Production Control teams ensure operations are adequately managed by maintaining and/or following documented operational instructions, managing and evaluating performance statistics over hardware and peripheral capacity utilization and performance, ensuring equipment is maintained on schedule, and ensuring a physical and logical segregation of source and object, test / development / production libraries.

ITD utilizes separate test and production environments critical systems. Some systems have separate development environments as well. New applications or application changes are tested by users in the separate test platform or region. After acceptance ITD system administrators and/or DBA migrate the changes to production.

Tests of Operating Effectiveness and the Results of Those Tests

We reviewed the operations checklists, IPL instructions, shut down procedures, and job restart procedures.

We interviewed ITD personnel regarding operations shifts and shift rotation procedures.

We reviewed ITD procedures for disposing of media and equipment.

The operations staff has established regular business hours. If operations receives a call outside of these regular hours, an automated voice response system notifies the on-call person. ITD schedules two employees for each shift so if someone is absent, they still have someone available.

The shut down procedures and job restart procedures are included in the IPL instructions. The IPL instructions were found in the operations room.

ITD uses software to write 0’s to hard drives and also uses a degasser on tapes and hard drives before disposing of them.

Conclusion

We conclude that ITD has met the objective of managing operations.

Objective – Ensure Compliance with External Requirements

To meet legal, regulatory and contractual obligations.

Controls

ITD manages its legal and contractual responsibilities and liabilities through ongoing internal monitoring of legislation, contracts, and regulatory changes.

ITD obtains independent assurance of compliance with laws, regulatory requirements and contractual obligations through audit functions conducted by the Office of the State Auditor. The State Auditor performs routine examinations of ITD's financial, performance, and IT controls.

ITD's Procurement Officer reviews RFP's and contracts for compliance with policies and procedures over hardware and software acquisition, implementation, and maintenance. State procurement rules govern the acquisition process - acquisitions must comply with state standards unless an exception is granted.

ITD utilizes the Attorney General standard contracts where possible, and has established service level agreements with key providers that provide contracted services to ITD. ITD's large-dollar contracts are reviewed and approved by the Attorney General. In addition, ITD follows the RFP and state procurement process.

Tests of Operating Effectiveness and the Results of Those Tests

We interviewed ITD personnel regarding how ITD identifies external requirements and ensures compliance with them.

ITD is reliant on agencies to notify them of legal and contractual requirements where ITD is responsible for compliance.

ITD identifies external requirements in two ways. For large projects or legislation that ITD is directly involved in, ITD is aware of these by their very nature. For legislation or contracts that other agencies are involved in the creation of, ITD becomes aware of these external requirements usually when the agency notifies ITD.

To ensure compliance with external requirements, ITD normally delegates the responsibility to the division director most affected by the requirements.

Conclusion

We conclude that ITD has met the objective of ensuring compliance with external requirements.

Objective – Managing Performance and Capacity

To ensure that adequate capacity is available and that best and optimal use is made of it to meet required performance needs.

Controls

ITD monitors computer and network operations performance based on assessments of individual systems and the knowledge of support and project teams, tools such as graphs, operators' knowledge, and available performance capacity system software. Performance management reports include e-mail messages by platform for e-mail servers, CPU utilization, DASD I/O per second, memory pages per second, and disk capacity for the mainframe.

ITD has implemented Mercury SiteScope infrastructure monitoring software over the state network platform to monitor performance characteristics (utilization, response time, usage and resource availability). ITD has configured SiteScope to automatically detect and report/record incidents over network resources.

ITD's Computer Systems Division has implemented ongoing procedures to monitor performance and capacity of the mainframe and mid-tier operating systems within the computer facility, and maintains historical statistics for future capacity planning and budgetary planning purposes.

Tests of Operating Effectiveness and the Results of Those Tests

We interviewed ITD personnel regarding how ITD monitors performance and capacity.

We reviewed the results of the most recent performance and capacity evaluation.

ITD uses Enterprise SiteScope to monitor the performance of critical systems. SiteScope monitors systems by periodically pinging them to determine if they are "alive". SiteScope also checks periodically to determine if applications are running. If SiteScope finds that the network or an application is down, it triggers an email, text message, or phone call (depending on the criticality of it) to the appropriate person. On the mainframe and AS/400, SiteScope only pings them. SiteScope does not check for applications that are still running on the mainframe or AS/400 because they have their own tools that do this.

We reviewed the AS/400 performance report for Feb, 2008. The report shows disk utilization for all storage pools along with CPU utilization. The report has statistics dating back from Feb, 2007. We reviewed the 2007-2008 email activity for ITD. This spreadsheet shows the numbers of changes in users for the year. There was a graph showing the different email platforms and the number of users.

We reviewed a file that showed outage avoidance statistics. This file shows unplanned and planned outages; along with what the outage was, the action taken, if there was any data loss, and how long the outage took.

Lastly we reviewed a spreadsheet for mainframe statistics. This file shows CPU utilization and disk capacity for taken from a period between 10-11a.m.

Conclusion

We conclude that ITD has met the objective of managing performance and capacity.

Objective – Assist and Advise Customers

To ensure that any problem experienced by the user is appropriately resolved.

Controls

ITD's Customer Service Division Support Center operates a help desk and provides a full-service central repository for customers to report problems, ask questions, request information, and receive back resolutions and answers in an organized and expedient manner.

ITD's Customer Service Division staff includes the Customer Service Director, Service Center Manager, one full-time Service Management Software Analyst and five full-time Service Desk Analysts. Service Desk Analysts cover 7am - 5pm M-F and rotate on-call Saturday morning through Monday 7am. Computer Operations staff cover calls 5pm - 7am M-F.

ITD's Support Center receives requests via telephone and email, and logs / tracks the requests through HEAT from FrontRange Solutions - Incident Management System. ITD has implemented HEAT with the following control parameters:
- Defined assignment groups, supervisors, and role-specific security
- Defined incident categories, call-types, sub-call-types, and incident priority matrix
- Defined detail screens to gather call-type specific information, and customer-specific details
- Acknowledgement, escalation, and communication procedures
- Monthly reporting & analysis, incident records archived 3 years

ITD's Customer Service Division performs monthly reporting and analysis of incident records (HEAT) and Automatic Call Distribution (ACD) telephone system records, and tracks performance measures based upon key indicators.

ITD's Customer Service Division has implemented the Continuous Improvement Cycle based upon IT Infrastructure Library (ITIL) best practices for Service Desks, Incident Management, and Change Management.

ITD's Computer Systems Division utilizes HEAT incident tracking system to address issues - escalation procedures are being followed and appropriate in resolving problems.

ITD conducts an annual customer survey to ensure the department is meeting customers' expectations. The survey allows customers to rate their satisfaction with the services provided by ITD and to suggestions for improvements. Survey areas are service desk, software development, network service, E-mail services, telephone services, application hosting, records management, IT planning and oversight services, and an overall ITD survey. Results are published in ITD's strategic plan and on ITD's website.

Tests of Operating Effectiveness and the Results of Those Tests

We interviewed ITD personnel regarding the registration of queries, escalation of those queries, and how queries are monitored and cleared.

We reviewed Help Desk policies and procedures.

We reviewed the latest performance measures for the Help Desk.

ITD help desk uses an incident management tool called HEAT, which was designed by Frontrange. HEAT provides an assignment guide to direct which ITD groups are to receive specific incidents and to solve the initial problem. ITD also uses the Information Technology Infrastructure Library (ITIL). ITIL is a set of concepts and techniques for managing information technology communications, development and operations. ITIL uses common terminology and basic concepts to break up technical problems into manageable modules.

ITD has an documented incident management process outline. This is an outline for the proper steps to be taken when an incident is reported. It contains a series of steps in the escalation of an incident to the second and third line of support.

The 2007 customer survey shows ITD's performance level in many different categories such as key performance indicators, overall services, overall coordination and oversight, overall attributes, service desk, software development, statewide network, email, telephone, application hosting, records management, statewide IT planning, statewide IT procurement, enterprise architecture, and enterprise project management. All of the areas are measured on a percentage scale from 'very satisfied' to 'very dissatisfied' in their overall performance, professionalism & courtesy, knowledge, timeliness, quality, and value. The 2007 customer surveys show that the majority of ITD's performance was rated at a 'satisfied' by the average number of respondents whom took the survey.

Conclusion

We conclude that ITD has met the objective of assisting and advising customers.

Objective – Determine Technological Direction

To take advantage of available and emerging technology to drive and make possible the business strategy.

Controls

ITD has established an Enterprise Architecture process. This process relies on participation of agency representatives. Each agency that is interested is invited to participate in various domain teams that study specific technology domains and provide proposals to the Architecture Review Board (ARB) and State Information Technology Advisory Committee (SITAC). This process addresses enterprise technology issues and results in state standards, policies and guidelines.

ITD is legislatively mandated to develop policies, standards, and guidelines for technology based on information from state agencies, institutions, and departments with the goal of creating a common statewide architecture. The Enterprise Architecture (EA) process promotes state agency participation with ITD in setting future direction of information technology in the state of North Dakota.

ITD publishes a quarterly agency newsletter titled "Information Link." ITD also coordinates the "IT Directional Meeting" for executive branch agency representatives to inform them on current initiatives and issues.

ITD's technological infrastructure is maintained on an ongoing basis, takes into account current and future technology trends and regulatory conditions, and is compared with the IT long and short range plans.

Tests of Operating Effectiveness and the Results of Those Tests

We reviewed the Enterprise Architecture process.

We interviewed ITD personnel regarding infrastructure planning.

Agencies are responsible for complying with IT Standards.

Enterprise Architecture is a process that provides an overall plan for designing, implementing and maintaining the underlying infrastructure to support information sharing and resource optimization. The concept of the Enterprise Architecture (EA) is to get agency participation and have more agencies buy into the process.

ITD produces the Statewide IT Plan that provides a high level view of infrastructure. ITD division directors initiate infrastructure changes by submitting business cases that are approved by ITD's management.

Conclusion

We conclude that ITD has met the objective of determining technological direction.

Objective – Define IT Organization and Relationships

To deliver the right IT services.

Controls

ITD is divided into seven divisions (Administrative Services, Software Development, Computer Systems, Telecommunications, Customer Service, IT Planning, Human Resources) to ensure authority and independence from user organizations.

Appropriate roles and responsibilities exist for key processes, including system development life cycle activities, (requirements, design, development, testing), information security, acquisition and capacity planning.

Per NDCC 54-59-07, the Statewide Information Technology Advisory Committee (SITAC) advises ITD regarding statewide IT planning, including providing e-government services for citizens and businesses, developing technology infrastructure to support economic development and workforce training, and developing other statewide IT initiatives and policy.

All data and systems in the custody of ITD have a defined owner. The defined owner is the agency responsible for the business results or the business use of the object. There is one and only one owner for each object.

ITD uses the ND Human Resource Management Services division job classifications for all positions, which detail the minimum qualifications necessary for each position. A position information questionnaire (PIQ) is used to further define the position qualifications and personnel selection criteria.

ITD's Human Resources Division has established policies and procedures for the evaluation and re-evaluation of IT position descriptions.

Tests of Operating Effectiveness and the Results of Those Tests

We reviewed legislation regarding ITD's setup and structure.

We reviewed ITD's organizational chart.

We reviewed ITD's data ownership policies and procedures. Agency security officers are responsible for controlling access rights.

North Dakota Century Code § 54-59-02 defines the duties and responsibilities of ITD.

Per NDCC 54-59-07 the state information technology advisory committee consists of the chief information officer; the commissioner of higher education or the commissioner's designee; the attorney general or the attorney general's designee; the secretary of state or the secretary of state's designee; the tax commissioner or the commissioner's designee; the chief justice of the supreme court or the chief justice's designee; two members of the legislative assembly appointed by the legislative council; a minimum of eight members representing state agencies, appointed by the governor; and two members with technology management expertise representing private industry, appointed by the governor.

ITD policy defines the owner as the agency responsible for the business results of the object, and there can be only one owner per object.

Conclusion

We conclude that ITD has met the objective of defining the IT organization and relationships.

Objective – Manage the IT Investment

To ensure funding and to control disbursement of financial resources.

Controls

ITD establishes the operating budget through the executive planning process (Budget Analysis & Reporting System) and manages budget v. actual expenditures through the centralized PeopleSoft accounting system. The budget is aligned with the enterprise strategic plan. Executive Branch agencies participate in preparing their portions of the IT plan. A goal of the process is to anticipate major infrastructure needs and plan accordingly.

The governor and state legislature set staffing levels biennially in ITD's budget. During the biennial budget process, ITD reviews staffing levels and requests additional FTE as needed.

ITD rate setting process and annual report include comparisons to similar rates charged by other states and private sector providers to ensure that the rates are competitive with similar services offered by other states and the private sector.

Tests of Operating Effectiveness and the Results of Those Tests

We reviewed ITD's appropriations bill for the 2005-2007 biennium

We reviewed ITD's Annual Report.

We reviewed ITD's budget vs. actual comparison.

ITD's appropriation bill HB 1021 contains five sections: Base Level Funding Information, Funding Adjustments or Enhancements Information, Appropriation, Transfers, and Borrowing Authority – E-rate Funding. Section 5: Borrowing Authority – E-rate funding states that ITD may borrow an amount necessary for certain telecommunications costs from the Bank of North Dakota upon the approval of the emergency commission.

Located within the annual report are the rate comparisons for network fees, telephone fees, long distance, and central computer CPU (rate based per second). Each area is compared with the surrounding or nearby states such as South Dakota, Minnesota, Montana, Wisconsin, and Nebraska. All rate comparisons shown for ITD seem to be competitive and reasonable.

ITD uses reports generated through PeopleSoft and Microsoft Excel spreadsheets to review the budget to actual.

Conclusion

We conclude that ITD has met the objective of managing the IT investment.

Objective – Communicate Management Aims and Direction

To ensure user awareness and understanding of those aims.

Controls

ITD organizational controls ensure appropriate and adequate resources are assigned to implement the organization's policies in a timely manner.

ITD procedures exist to address the need to periodically review and approve key standards, directives, policies and procedures relating to information technology.

ITD management promotes a positive control environment by example and has accepted full responsibility for formulating, developing, documenting, promulgating, controlling and regularly reviewing policies governing general aims and directives.

ITD evaluates the internal control processes within the department on an ongoing basis, through management meetings, budgetary review, external audits - including SAS70 reviews, internal security assessment, and through internal assessment of policies and procedures.

ITD management and staff meet on a scheduled basis to discuss internal operations and direction. Managers and supervisors meet weekly, and all ITD staff meet twice per year.

On an annual basis, ITD employees are required to sign an Acknowledgment of Secrecy Provision to ensure they are aware of the confidentially requirements of the data they handle. In addition there is an annual acknowledgement of seven other policies relevant to the department.

ITD performed criminal background checks on all employees and recorded fingerprints in June 2003. ITD performs an annual update of the employee information and has defined procedures to perform follow-up background checks on the employees every five years. The Bureau of Criminal Investigations is contracted to perform this service for ITD.

ITD policies and procedures are published and made available to ITD employees on the intranet.

Tests of Operating Effectiveness and the Results of Those Tests

We interviewed ITD personnel regarding how ITD develops and maintains their policy manual and how they ensure adequate resources are assigned to implement the policies.

We reviewed ITD's policy manual.

We reviewed minutes from ITD's meetings with employees to determine if they communicate and train staff regarding the control environment.

Potential policy and procedures manual changes can come from issues raised at staff meetings, exit interviews, employee surveys, and through a formal process where changes are submitted to human resources. The Employee Policy Council, made up of the directors and some human resources personnel, meets quarterly to specifically discuss potential policy changes. Policy changes are approved by this council. If the council approves the changes, they update the manual, and send and e-mail to ITD staff informing them of the changes made to the manual. The policy and procedure manual is kept on ITD's intranet.

The policy manual was last updated December 17, 2007. The manual includes policies addressing integrity, ethical values, code of conduct, security and internal controls, competence of personnel, and management philosophy and operating style. Policies relating to quality of services are mentioned as part of the mission and vision and are mentioned briefly in the general rules of conduct. For most policies, the reason for the policy is detailed. The policy manual also explains the different types of disciplinary actions that may be taken and when those actions should be used.

Conclusion

We conclude that ITD has met the objective of communicating management aims and direction.

Objective – Assess Risks

To support management decisions through achieving IT objectives and responding to threats by reducing complexity, increasing objectivity and identifying important decision factors.

Controls

ITD manages risks associated with individual procurement contracts based on the dollar value and by requiring agencies to provide documented requests for information technology.

Tests of Operating Effectiveness and the Results of Those Tests

We interviewed ITD personnel regarding how ITD assesses risks, responds to risk identified, and updates the risk assessment over time.

ITD considers IT risks in an ad hoc manner. In the areas of security and disaster recovery ITD has developed good processes and controls that suggests that a risk assessment was done, however; the risk assessment was not documented.

Finding: ITD lacks a formal risk assessment framework

While critical business processes have been identified, there is not a systematic approach to identifying, assessing, and mitigating or accepting risks to those business processes. Such a framework should incorporate a regular assessment of the relevant information risks to the achievement of the business objectives, forming a basis for determining how the risks should be managed to an acceptable level. Management should ensure that reassessments occur and that risk assessment information is updated with results of audits, inspections and identified incidents. Without a formal risk assessment process management may not have adequate information to make sound decisions in the use of assets to mitigate risks.

Recommendation

We recommend the Information Technology Department develop a systematic risk assessment framework.

ITD Response

ITD agrees with the recommendation and plans to leverage our relationships with other security organizations in other states to determine best practices in this area.

Conclusion

We conclude that though risk assessments are done in an ad hoc manner, ITD has met the objective of assessing risks.

Objective – Managing Projects

To set priorities and to deliver on time and within budget.

Controls

North Dakota Century Code Section 54-35-15.2 provides that the Legislative Information Technology Committee shall "review the cost-benefit analysis of any major information technology project (=> 250K per biennium or => $500K in total) of an executive or judicial branch agency" and "perform periodic reviews to ensure that a major information technology project is on its projected schedule and within its cost projections."

ITD's large project reporting has five phases: business case, project plan, quarterly status reports, summary status report, and post-project analysis. In the business case phase the agency defines the business requirements, does a cost/benefit and risk analysis, establishes a project manager and executive steering team, and presents this to the Legislative Information Technology Committee. ITD has established guidelines for making the business case. The project plan is to be prepared based on industry "best practices." ITD encourages the use of the Project Management Institute (PMI) format. Quarterly reports define the scope of the project and state the project schedule. The report compares budgeted to actual costs and outlines current progress and issues. ITD's planning analysts review the report and present summary status reports to the Legislative Information Technology Committee each quarter. The post-project analysis assesses whether the project accomplished its business objectives.

ITD's large project oversight process ensures the project plan includes a formal system development life cycle for system development and installation, including requirements definition, coding, testing, conversion, training, and documentation.

ITD's large project oversight process incorporates quality management processes within the project plan.

Tests of Operating Effectiveness and the Results of Those Tests

We reviewed legislation regarding project management.

We reviewed ITD's project management and large project guidelines.

We interviewed ITD personnel regarding how ITD monitors large projects.

We reviewed the latest large project status report.

The information technology committee should receive and review information pertaining to the project description, project objectives, and the cost –benefit analysis of any major information technology project of an executive or judicial branch agency. They should also review to ensure the technology project is on its projected schedule and within cost projections. A major project is a project with a cost of two hundred fifty thousand dollars or more in one biennium or a total cost of five hundred thousand dollars or more.

The information technology committee may review any project and if it's determined that the project is at risk of failing to achieve its intended result, the committee may recommend to OMB the suspension of the funds for the project. OMB has the right to suspend the funds if they agree with the recommendation of the committee.

ITD shall prepare and present an annual report to the information technology committee which contains a list of all projects for which financing agreements have been executed.

During the life of the project, if any project goes more than 20% over scheduled or over budget they need to notify the state information technology advisory committee. Also upon completion of the project, if any project exceeded more than 20% over the original budget or over scheduled completion date they need to notify the state information technology advisory committee.

The North Dakota State Project Management Guidebook was created to provide a common methodology for managing projects within state government. The guidebook is designed to supply enough detail to guide new project managers through the project management process. Also the guidebook provides guidance for agency staff to use when contracting with private vendors.

When a new large project is proposed, a business case must be submitted to ITD through email. The business case needs to be submitted to ITD prior to any pre-project expenditure's. ITD will then review the business case to make sure the information above is thoroughly explained and provide comments within ten business days of receipt. Once the business case has been finalized, a final copy is sent to the Legislative Council.

The next process is to develop a project charter. A project charter minimally needs to include a project background, project scope, project objectives, critical success factors, required resources, constraints, assumptions, and project authority. The project charter needs to be completed prior to the planning process. Once completed, the project charter is sent to a project sponsor for approval. After the approval, an Executive Steering Committee is established to help support the management of the process. The committee will meet quarterly and is responsible for reviewing project milestones, authorizing significant changes, and facilitating decision-making.

A project plan is developed as a primary planning document for the project. The project plan should identify specific milestones throughout the project along with their associated cost, schedule, and deliverables. Once completed, the project plan is sent to the project sponsor for approval. A copy is sent to ITD upon approval from the project sponsor.

A project status report is created and submitted to ITD. The project status report should include an executive summary, budget schedule, issues, risks, project accomplishments, and upcoming events. The project status report needs to be submitted to ITD on a quarterly basis or when a milestone exceeds twenty percent of planned cost or schedule.

Upon completion of the project, a Post Implementation Review (PIR) is performed and a closing report is created by the agency to assess the success of the project and to capture historical information. A copy of the PIR and closing report are sent to the Legislative Council.

We reviewed the Large Project Summary Report for the period ending September 30, 2007. During this period, 6 projects were reported in the planning stage, 4 projects moved into the execution phase, and 3 projects were reported complete. The 3 completed projects show if they were over/under budget and how the schedule of the project turned out. There are 5 projects that reported budget/schedule variances and those are being monitored closely.

We reviewed the Active Large Project Summary Report for the period ending September 30, 2007. There were 17 projects that were active.

Conclusion

We conclude that ITD has met the objective of managing projects.

Objective – Manage Changes

To minimize the likelihood of disruption, unauthorized alterations, and errors.

Controls

ITD completed deployment of the Work Management System (WMS) to state agency users in November 2004. ITD developed this web-based system internally to provide a "one-stop center" for customers to request ITD software development services, and enhance ITD's project management, time recording, and billing services.

ITD's Computer Systems Division database administrators use the Work Management System to track customer change requests and document software changes over Websphere, .NET, and agency database applications maintained by ITD.

ITD manages changes to application software by documenting, prioritizing, and tracking system changes requests from users. The change process is monitored by ITD for improvements in acknowledgment, response time, response effectiveness and user satisfaction with the process.

ITD utilizes a formal SDLC methodology to develop and maintain applications for its customers. This methodology includes peer reviews and load testing for quality assurance purposes.

ITD Distributed Systems utilizes a web-based change management system to log changes. Changes are logged in the system and approved by the Computer Systems Manager or the System Architect.

Tests of Operating Effectiveness and the Results of Those Tests

We interviewed ITD personnel regarding how ITD tracks and authorizes changes.

The majority of change requests are initiated by the end user through ITD's Work Management System. System administrators can access the application to request a change. The application records the User ID of the requestor and the time and date of the request automatically. The requestor must fill in a title for the change request, the category of the change, the date the change needs to be made by, and a detailed description of the change. When this is submitted, an e-mail is sent to Computer Systems Manager to notify them of the change request. The Computer Systems Manager then must access the application and approve or deny the change request.

Conclusion

We conclude that ITD has met the objective of managing changes.

Objective – Identify and Allocate Costs

To ensure a correct awareness of the costs attributable to IT services.

Controls

ITD sets its rates to cover the cost of providing services with a reasonable surplus to finance capital purchases. ITD monitors actual expenditures to billings through the PeopleSoft accounting system cost centers with the goal of matching billings to expenditures within each cost center.

ITD's strategic planning process outlines the rates and funding mechanisms necessary to finance the proposed activities of the department, in accordance with NDCC 54-59-06.

Tests of Operating Effectiveness and the Results of Those Tests

We interviewed ITD personnel regarding how ITD sets rates.

We reviewed ITD’s Strategic Business Plan for rate information.

We reviewed the rate setting system to ensure it recovers the costs of IT services.

All of the ITD rates are billed into three different categories, Data Processing, Telecommunications, and Micrographics. On the ITD website each of these three different categories are broken down into types of services and has a short description for each specific type of service that is being provided. Each biennium ITD needs to adjust rates for most of their services provide. These adjustments are to cover costs that include increases for professional staff, health insurance premiums and software maintenance. Each rate is set in the hope that is will not have to be adjusted during the biennium due to the set budgets created by each agency. ITD also monitors what other entities are charging for similar services so that they can maintain fair prices.

ITD’s annual report compares rates to the different prices in neighboring states (South Dakota, Montana, Wisconsin, and Minnesota).

ITD also does financial statement and analytical review every month. Every month, they prepare a cost center statement that shows how each cost center is performing. They look at what the trend is for each cost center, whether it is over-recovering and under-recovering. They also prepare a cash flow projection where they look at any large payments that need to be made in the future.

Conclusion

We conclude that ITD has met the objective of identifying and allocating costs.

Objective – Define a Strategic Information Technology Plan

To strike an optimum balance of information technology opportunities and IT business requirements as well as ensuring its further accomplishment.

Controls

ITD publishes an annual report which includes: major accomplishments; ITD's performance against goals; ITD's service rates (rates that generate 90% of ITD revenue) which are compared with costs charged by similar organizations; the strategic planning process; an update on internal performance measures, and future IT initiatives. ITD distributes the report to the Legislative Information Technology Committee, Legislative Audit and Fiscal Review Committee and Senior Information Technology Committee. The report is also available at ITD's website under "Publications".

ITD meets with key customers on a monthly or quarterly basis to gather information about future plans and needs.

ITD maintains a biennial Strategic Business Plan, outlining goals and objectives for the department, and follows a methodology for measuring progress toward the goals outlined in the business plan, per NDCC 54-59-06.

ITD evaluates progress toward the goals outlined in the strategic plan, and publishes the results in the annual report (balanced scorecard). ITD also tracks performance metrics internally, both at the department and division levels.

ITD's strategic planning process takes into account organizational changes, technology evolution, regulatory requirements, business process reengineering efforts and staffing requirements.

ITD provides guidelines for agencies to follow in preparing their technology plan, reviewing the plans for compliance with statewide policies or standards, resolving conflicting directions among plans, and assembling the agency plans into a statewide plan to be submitted to the members of the Legislative Assembly. ITD also reviews and approves technology acquisitions for conformance with the agency's IT plan and compliance with statewide policies and standards.

ITD's annual customer survey includes a section on information technology planning. ITD's Information Technology Planning Analyst reviews the surveys and meets with agencies to assess the IT planning process.

State agency IT Plan updates are to be done as needed to communicate the IT direction and resource needs of the agency. The IT plan must be updated if the goals and objectives change, if a major project is added or deleted, or at the request of ITD.

ITD surveys internal employees to identify and assess any performance issues and establish internal goals / objectives.

Tests of Operating Effectiveness and the Results of Those Tests

We reviewed ITD's most recent Strategic Business Plan, Annual Report, and Statewide IT Plan.

We interviewed ITD personnel regarding how ITD establishes the annual report and strategic plan.

We interviewed ITD's personnel regarding meetings with key customers.

We reviewed the agency IT planning process which ITD oversees.

ITD prepares a biennial Strategic Business Plan and an Annual Report. The Strategic Business Plan outlines ITD's vision, goals, and objectives, the plan appeared to be consistent with the business goals of the State of North Dakota. The Annual Report measures ITD's performance but includes only selected performance measures. ITD meets monthly to discuss the Strategic Business Plan and progress towards objectives.

ITD personnel indicated that meetings with key customers occur. We reviewed agendas from past meetings; no minutes are kept from these meetings.

The duty for defining the form of biennial agency IT plans has been assigned to ITD. ITD has established guidelines for agency plans and has a process set up to assist agencies in their planning. ITD reviews finished plans for completeness and adherence to the guidelines.

Conclusion

We conclude that ITD has met the objective of defining a strategic information technology plan.